What is claimed is:

1. A method for generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message, $0 \leq M \leq n-1$, n is a composite number formed from the product of a number k of distinct random prime factors $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2, and $S \equiv M^d \pmod{n}$, comprising the steps of:

a first individual in a group performing a first partial digital signature subtask on a message M using a first individual private key to produce a first partial digital signature S_1;

at least a second individual in said group performing a second partial digital signature subtask on said message M using a second individual private key to produce a second partial digital signature S_2; and

combining said partial digital signature results including said results S_1 and S_2 to produce the group digital signature S corresponding to said message M.

2. A method for generating a group digital signature as recited in claim 1 wherein said step of combining said results associated with said first and second partial digital signatures includes:

combining said results in accordance with a Chinese Remainder Algorithm.

3. A method for generating a group digital signature as recited in claim 1 wherein each of said individual private keys includes,

an associated individual modulus n_i that is a number formed as a product of one or more of said k prime factors of said group modulus n, and

an associated individual private exponent d_i that is determined based on a selected public group exponent e, and also based on the prime factors of said associated individual modulus n_i.

4. A method for generating a group digital signature as recited in claim 3 wherein each of said individual private exponents d_i is determined as a number congruent to the inverse of said public group exponent e, modulo the Euler Totient function of said associated individual modulus n_i.

5. A method for generating a group digital signature as recited in claim 1 wherein the first individual is assigned a first number m_1 of the k prime factors of said group modulus n and the second individual is assigned a second number m_2 of the k prime factors of said group modulus n, and wherein:

said first individual private key includes,

an associated individual modulus n_1 that is determined as the product of a number m_1 of distinct prime factors of said group modulus n, and

an associated individual private exponent d_1 that is determined based on a selected public key exponent e and based on the m_1 prime factors of said associated individual modulus in accordance with

$d_1 \equiv e^{-1} \bmod (\prod_{j \le m_1} (p_j \quad 1))$, wherein $p_1 \ldots p_{m1}$ represent the first number m_1 of said distinct prime factors.

6. A method for generating a group digital signature as recited in claim 3 wherein said first partial digital signature S_1 is generated based on the relationship

$$S_1 \equiv M^{d_1} (\mathrm{mod}\ n_1).$$

7. A method for generating a group digital signature as recited in claim 1 wherein said first individual private key is created based on associated prime factors p_a and p_b of the group modulus n, said first individual private key including,

an individual modulus n_1 that is a composite number formed as the product $p_a \cdot p_b$ of said associated primes, and

an associated individual private exponent d_1 that is determined based on a selected public key exponent e and said associated primes p_a and p_b in accordance with

$$d_1 \equiv e^{-1} \bmod ((p_a-1)(p_b-1)).$$

8. A method for generating a group digital signature as recited in claim 7 wherein said first partial digital signature S_1 is generated based on the relationship,

$$S_1 \equiv M^{d_1} (\mathrm{mod}\ n_1).$$

9. A method for generating a group digital signature as recited in claim 2 wherein the group comprises z individuals whose private key moduli n_i are relatively prime, wherein said step of combining results of said sub-tasks is performed in accordance with the relations

$$Y_i \equiv Y_{i-1} + ((S_i - Y_{i-1})\ (w_i^{-1} \bmod n_i) \bmod n_i) \bullet w_i \bmod n,$$

wherein $2 \leq i \leq z$, and

$$S = Y_k,\ Y_1 = S_1, \text{ and } w_i = \prod_{j<i} n_j.$$

10. A method for generating a group digital signature as recited in claim 2 wherein the group comprises z individuals whose private key moduli n_i are relatively prime, wherein said step of combining results of said sub-tasks is performed in accordance with the relations

$$S \equiv \sum_{i=1}^{z} S_i (w_i^{-1} \bmod n_i) w_i \bmod n,$$

wherein

$$w_i = \prod_{j \neq i} n_j.$$

11. A method of creating and assigning individual private keys to each member of at least one group of individuals, wherein the individuals in each group may use their assigned keys to sign a message M to collectively create a group digital signature S associated with an entity that includes all of the groups, wherein M corresponds to a number representative of a message, $0 \leq M \leq n-1$, n is a composite number formed from the product of a total number k of distinct random primes $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2, and $S \equiv M^d \pmod{n}$, and wherein each such group of individuals collectively control all of the primes, but wherein no single one of the individuals controls all of the prime factors $p_1, p_2, \ldots p_k$, comprising:

assigning at least one of the total number k of prime numbers $p_1, p_2, \ldots p_k$ to each of a plurality of members of each of at least one group, wherein all of the prime numbers assigned to the individuals within each group are distinct;

defining a unique individual modulus associated with each of the individuals formed as the product of the prime numbers assigned to the individual; and

defining a unique individual private key for each of the individuals based on the associated individual modulus formed for the individual;

whereby each of the individual private keys may be used to create an associated individual partial digital signature, wherein the individual partial digital signatures of the members of a group may be combined to form the group digital signature S, and wherein at least one of the partial digital signatures cannot be combined across different groups to form the group digital signature S.

12. A method of creating and assigning individual private keys as recited in claim 10 wherein the keys are created and assigned in accordance with a symmetric distribution of the k prime factors of n, wherein each of the individual members of a group is assigned an individual private key based on a modulus formed as a product of m distinct prime factors, and wherein m < k.

13. A method of creating and assigning partial digital signature keys as recited in claim 11 wherein the number of combinations of the k prime factors taken m at a time dictates the number of distinct individual private keys that may be created based on the total number k prime factors, and wherein the number of combinations of k prime factors taken m at a time is expressed in accordance with

$$A = \binom{k}{m} = \frac{k!}{m!(k-m)!}$$

and wherein said individual private keys are organized into $g = A/z = A \cdot m/k$ groups comprising $z = k/m$ members in each group.

14. A method of creating and assigning individual private keys as recited in claim 10 wherein the keys are created and assigned in accordance with an asymmetric distribution of the k prime factors of n, wherein at least one of the individual members of a group is assigned an individual private key based on a modulus formed as a product of m_1 distinct prime factors, and wherein at least one other member of said group are assigned individual private keys each based on a modulus formed as a product of m_2 distinct prime factors, wherein $m_1 < m_2 < k$.

15. A method of creating and assigning individual private keys as recited in claim 13 wherein the keys are created and assigned in accordance with an asymmetric distribution of the k prime factors of n, wherein at least one private key is assigned across more than one group.

16. An apparatus for generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message, $0 \leq M \leq n-1$, n is a composite number formed from the product of a number k of distinct random prime factors $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2, and $S \equiv M^d \pmod{n}$, comprising:

a secure key generation facility;

a plurality of individual secure private key storage and signing entities; and

a secure group signature combining entity.

17. An apparatus for generating a group digital signature as recited in claim 14, wherein the secure key generation facility and secure group signature combining entity are combined within a common security boundary.

18. An apparatus for generating a group digital signature as recited in claim 14, including:

means for transferring individual private keys generated by the secure key generation facility into secure tokens for issuance to the assigned individual users of said private signing keys, and

means for securely transferring associated secret group combining parameters from the secure key generation facility to the secure combining entity.

19. An apparatus as recited in claim 14 wherein each of said tokens is a smart card.